



DOCKET FILE COPY ORIGINAL

**U.S. Department of Justice**

Federal Bureau of Investigation

*Telecommunications Industry Liaison Unit  
P.O. Box 220450  
Chantilly, VA 20153-0450*

March 10, 1998

EX PARTE OR LATE FILED

**RECEIVED**

MAR 10 1998

FEDERAL COMMUNICATIONS COMMISSION  
OFFICE OF THE SECRETARY

Ms. Magalie R. Salas  
Secretary  
Federal Communications Commission  
1919 M Street, N.W.  
Room 222  
Washington, D.C. 20554

Re: The Federal Bureau of Investigation's (FBI) and Law Enforcement's Ex Parte Presentation Regarding the Communications Assistance for Law Enforcement Act, Notice of Proposed Rulemaking, CC Docket No. 97-213, FCC No. 97-356, (rel. October 10, 1997).

Dear Ms. Salas:

Pursuant to Section 1.1206(b)(2) of the Commission's rules, 47 C.F.R. § 1.1206(b)(2), this letter is to advise the Commission that, in connection with the above-referenced rulemaking proceeding, Mr. Rajesh Puri, Mr. Brandon Ritchey, Mr. Michael T. McMenamin and I, met with Mr. Kent Nilsson, Mr. Marty Schwimmer, and Mr. David Ward from the Commission's Common Carrier Bureau; Mr. Charles Iseman, Mr. Lawrence Petak and Mr. Jim Burtle from the Commission's Office of Engineering and Technology, in which the Communications Assistance for Law Enforcement Act (CALEA) was discussed. The Federal Bureau of Investigation (FBI) is filing this ex parte letter in order to summarize the substance of its March 9, 1998 meeting with Commission staff.

The FBI's oral ex parte presentation included a simulator demonstration of the nine (9) capabilities that have been identified by the FBI as necessary to support electronic surveillance, but are missing from the industry's interim standard, J-STD-025. In the meeting, the FBI stated its professional opinion as to why the nine (9) capabilities are essential in regards to Law Enforcement's ability to effectively effectuate electronic surveillance as prescribed under Section 103 of CALEA, 47 U.S.C. § 1002. The following is a short concise summary of the nine (9) missing capabilities and the FBI

No. of Copies rec'd 2  
List ABOVE

distributed this summary to Commission staff at its meeting.

**Capability #1: Content of conference calls.** Law enforcement needs to receive all conversations between two or more parties over a subject's conference facilities. That supports the primary intent of a Title III interception to access and deliver all communications supported by the subject's equipment, facilities, or services. Now, J-STD-25 only requires communications from a conference call to be delivered to law enforcement when the subject's terminal is connected to the subject's conference. Criminal subjects often use other terminals to call their own telephone number to use their services. The carrier has no way of knowing which human being is the subject and should deliver the communications throughout the duration of the conference.

**Capability #2: Party Hold, Party Join, and Party Drop Messages.** The intent of these messages is to be able to identify who is in the subject's conference at any time during the conference. Knowing when each participant to a call joins or departs the call enables law enforcement to know the source and recipient of each communication within the call. Without those messages, law enforcement would not know who joins or leaves a conference. Law enforcement would not know if the subject alternates between calls. Law enforcement would not know who said or heard what part of a conversation. By providing incomplete call-identifying information, the industry would deny evidence that parties had remained on the call after they first joined. The lack of such evidence allows doubt to be raised as to whether a party participated in subsequent communications in the call and jeopardizes any prosecution based on that evidence, risking violent criminals returning to the streets.

**Capability #3: Access to subject-initiated dialing and signaling.** Law enforcement needs to know all of the subject's input to the network throughout each call to understand how the subject directs the communications. Without such information, law enforcement would not know what keys a subject pressed to control calls to or from the subject's service. Law enforcement and carriers would be unable to testify in court on such fundamental issues as whether the subject was still involved in the call, in what fashion is the subject involved in the call, and how does the subject control his services related to the call or separate from the call.

**Capability #4: Notification Messages for in-band and out-of-band signaling.** Law enforcement needs to know what network information is sent to the subject or associates from the subject's service throughout each call. Such information tells the subject and law enforcement whether a particular directive by the subject or associate results in the establishment of a call, a redirection or modification of the call, or how the call terminates or releases. Law enforcement would not know what information the network provides the subject about calls to associates and would not know what information the subject's service provides to associates. That information often causes the subject or associate to take a particular course of action which may prove crucial as to why and how events took place.

---

**Capability #5: Timely delivery of call data.** Law enforcement needs to be able to associate call data with call events. Furthermore, call data must be delivered in time to be useful during emergency situations. Now, J-STD-25 places no requirements on when call data is to be delivered. Law enforcement is asking that call data be delivered to law enforcement within a specified time after a call event comparable to the speed with which other signaling messages are sent in the public network. Without such a requirement, law enforcement could not clearly associate call data with the correct call, raising doubts about the validity of the evidence. Timely data would also permit quick reaction to situations where the lives are threatened of law enforcement agents, innocent victims, or even the criminals themselves. Life-saving action may be delayed until call data can identify who is involved and their whereabouts.

**Capability #6: Surveillance Status Message.** The receipt of that message would indicate that the interception software is working correctly and is accessing the subject rather than an innocent subscriber. It would also confirm that the path over which the message was sent was still operational. Without this capability, law enforcement would not know when the software is turned on or off, or if it has failed. Law enforcement could not verify that the subject is being monitored until a call is received, leaving open the possibility that important evidence has been lost. Providing this message will enable law enforcement to quickly correct any faults in the implementation of an interception.

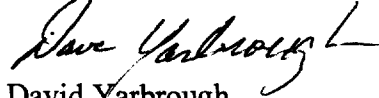
**Capability #7: Feature Status Message.** That message reports when a subject's capabilities change, even when the subject modifies capabilities remotely through another phone or an operator unaware of an interception. Law enforcement's capability to intercept may not match the subject's capability. Evidence may be lost if lines to law enforcement are unavailable. Manual methods would not be cost-effective for either law enforcement or the carriers. Cellular carriers in particular already have a need to pass such information between a home and visited switch and have already incorporated such a capability in their signaling messages.

**Capability #8: Continuity Check.** A continuity check capability would verify that a link between the carrier and law enforcement works. The intent is to enable law enforcement to know when a communications delivery circuit has failed as opposed to being available for service but idle. Uncorrected failures would mean loss of evidence that could be crucial to the case.

**Capability #9: Dialed Digit Extraction.** Extracting dialed digits from the communications path and delivery of all dialed digits over a single line to law enforcement results in a cost-effective use of circuits for both law enforcement and the carriers. When calls are set up in steps through multiple carriers, such as for toll-free numbers and collect calling numbers, law enforcement would not get all digits on one line. The initial dialing would be delivered as data, while the industry has proposed delivering dialing to subsequent carriers by providing the call content. Law enforcement does not want to have to lease two different lines to receive all dialing information and does not want to have the responsibility of separating dialed digits from content, which prompts privacy concerns.

In accordance with Section 1.1026(b)(2), Law Enforcement has hereby summarized its ex parte oral presentation of March 9, 1998, to Commission staff regarding the above-referenced proceeding. Any questions regarding this notice should be addressed to the undersigned.

Sincerely,

A handwritten signature in dark ink, appearing to read "Dave Yarbrough", with a stylized flourish at the end.

David Yarbrough  
Supervisory Special Agent  
Federal Bureau of Investigation

Enclosure

cc: Mr. Charles Iseman  
Mr. Kent Nilsson  
Mr. Lawrence Petak  
Mr. Marty Schwimmer  
Mr. David Ward  
Mr. Jim Burtle